MS 3.2 Management Services Functional Requirements

Management Services will incorporate the following functions for managing the network, system, and security of DII: Configuration Management, Fault Management, Performance Management, and Security Management. The requirements for these functions are specified in the following subsections:

- MS 3.2.1 Configuration Management
- MS 3.2.2 Fault Management
- MS 3.2.3 Performance Management
- MS 3.2.4 Security Management

The DII COE will employ an integrated management perspective for the individual DII sites. Management will be performed within a defined set of management domains, in accordance with the DII System and Network Management Concept of Operations. Network management of the Defense Integrated Services Network (DISN) Secret Internet Protocol (IP) Router Network (SIPRNET) WAN will be performed separately by the Defense Information Systems Agency (DISA).

MS 3.2.1 Configuration Management

Configuration Management includes functions to control the configuration of network, system or application entities. Configuration Management will provide automated tools for identifying, controlling and collecting data on DII resources for the purposes of determining status, user account management and auditing. These automated tools shall be available from any host as needed and as appropriate within the administrative domain. Additionally, these automated tools shall support multiple, simultaneous access by authorized administrators. Supporting this area are the functions to:

1. Create, delete, examine and change sets of management information that describe parts of a system.
2. Examine and be notified of changes in the state of the system to monitor overall operability and use of the system and give or withhold permission for the use of specific resources.
3. Examine the relationships among various parts of the system to see how the operation of one part of the system depends upon or is depended upon by other parts.

Configuration Management incorporates the following requirements for network, system and security components as it applies.

3.2.1.1 Management Services shall comply with account group requirements as specified in the DII I&RTS. Account Groups are a set of logically related system functions provided by one or more COE segments. COE segments may provide system functions for one or more account groups.

Traceability:
Priority ???

3.2.1.2 Management Services will support a master profile which defines the user configuration for all of the system functions contained within a base account group.

Traceability:
Priority ???

3.2.1.2a The master profile shall be used as a template to create other profiles within an account group.

Traceability:
Priority ???

3.2.1.2b The master profile shall not be assignable to a user, only those profiles that are created from the master profile template are assignable to users. Profiles may contain all or a subset of the system functions within a base account group.

Traceability:
Priority ???

3.2.1.2c Profiles shall only contain system functions from one account group.
Traceability:
Priority ???

3.2.1.2d The user's active profile(s) shall control the user's access to system functions within the user's session.
Traceability:
Priority ???

3.2.1.3 Management Services shall provide a GUI-based capability for centralized profile creation with the capability to define the following parameters:

- Unique Profile Name (within administrative domain)
Traceability:
Priority ???

- Account Group
Traceability:
Priority ???

- System Function(s)
Traceability:
Priority ???

3.2.1.3a The profile creation mechanism shall require the definition of the profile name and account group, as a minimum, in order to create the new profile.
Traceability:
Priority ???

3.2.1.3b The definition of the system function(s) shall be optional.
Traceability:
Priority ???

3.2.1.4 The profile creation mechanism shall provide the capability to create new profiles from existing profiles, e.g., a "save-as" capability.
Traceability:
Priority ???

3.2.1.5 The profile creation mechanism shall be extensible such that it will support the execution of additional tasks during profile creation as required by the COE and its segments. These tasks may include the creation of a profile-based mail group, mail box and routing mechanism.
Traceability:
Priority ???

3.2.1.6 The profile creation mechanism shall be extensible such that it will support the execution of additional tasks during the assignment of a system function to a profile as required by the COE and its segments. These tasks may include the assignment of database privileges to a profile.
Traceability:
Priority ???

3.2.1.7 The profile creation mechanism shall be extensible such that it will support the execution of additional tasks during the deassignment of a system function to a profile as required by the COE and its segments. These tasks may include the deassignment of database privileges to a profile.
Traceability:
Priority ???

3.2.1.8 Management Services shall provide a GUI-based capability for centralized profile modification with the capability to modify the following profile parameters:

- System Function(s)

Traceability:
Priority ???

3.2.1.9 Management Services shall provide a GUI-based capability for centralized profile deletion. The profile deletion mechanism shall reverse all actions associated with profile creation including deassigning the deleted profile from all users who have been previously assigned the deleted profile.
Traceability:
Priority ???

3.2.1.10 The profile deletion mechanism shall be extensible such that it will support the execution of additional tasks during profile deletion as required by the COE and its segments. These tasks may include the deletion of a profile-based mail group, mail box and routing mechanism.
Traceability:
Priority ???

3.2.1.11 Management Services shall provide a GUI-based capability for centralized assignment of profile(s) to users with the capability to define the following parameters:

- User Identifier

Traceability:
Priority ???

- Profile(s)

Traceability:
Priority ???

3.2.1.12 The profile assignment mechanism shall be extensible such that it will support the execution of additional tasks during user profile assignment as required by the COE and its segments. These tasks may include adding a user to a profile-based mail group.
Traceability:
Priority ???

3.2.1.13 Management Services shall provide a GUI-based capability for centralized deassignment of profile(s) to users. The profile deassignment mechanism will provide the capability to reverse all actions associated with assignment of profile(s) to users.
Traceability:
Priority ???

3.2.1.14 The profile deassignment mechanism shall be extensible such that it will support the execution of additional tasks during user profile deassignment as required by the COE and its segments. These tasks may include deleting a user from a profile-based mail group.
Traceability:
Priority ???

3.2.1.15 Management Services shall provide the capability to automatically distribute or make available profile information to a single host, a group of hosts or all hosts within the administrative domain.
Traceability:

3.2.1.16 Management Services shall provide a GUI-based profile selection mechanism with the following capabilities:
Traceability:
Priority ???

3.2.1.16a The profile selection mechanism shall be available after successful user login should the user possess multiple profiles and the ability to select multiple profiles. The presentation of

the profile selection mechanism shall be configurable such that it may be disabled by the administrator.

Traceability:
Priority ???

3.2.1.16b The profile selection mechanism shall be available in the user's work environment to allow dynamic changing of profiles such that users may select additional profiles and deselect previously selected profiles.

Traceability:
Priority ???

3.2.1.16c The profile selection mechanism shall display the user's valid profiles, currently selected profile(s) and unselected profile(s).

Traceability:
Priority ???

3.2.1.16d The profile selection mechanism shall allow a configurable number of selections, either 1 or n, where the user may be restricted to selecting one profile only or can select any number of profiles up to n where n is the total number of valid profiles for the user.

Traceability:
Priority ???

3.2.1.16e The profile selection mechanism shall allow an administrator to restrict the occupancy of a profile to one user in an administrative domain, e.g., the capability to lock a profile on a profile by profile basis.

Traceability:
Priority ???

3.2.1.17 The profile selection mechanism shall be extensible such that it will support the execution of additional tasks during user profile selection as required by the COE and its segments. These tasks may include providing the user with database access privileges based on the assumption of a profile.

Traceability:
Priority ???

3.2.1.18 The profile selection mechanism shall be extensible such that it will support the execution of additional tasks during user profile deselection as required by the COE and its segments. These tasks may include removing the user's database access privileges based on the deselection of a profile.

Traceability:
Priority ???

3.2.1.19 Management Services shall provide a GUI-based capability for centralized user account creation in a heterogeneous environment with the capability to define the following user parameters:

- Unique user identifier (within administrative domain)

Traceability:
Priority ???

- Login name

Traceability:
Priority ???

- Initial password

Traceability:
Priority ???

- Home directory file server

Traceability:
Priority ???

- Group memberships

  Traceability:
  Priority ???

- Mail alias(es)

  Traceability:
  Priority ???

- Shell

  Traceability:
  Priority ???

- Other user information, e.g., user's real name, telephone

  Traceability:
  Priority ???

3.2.1.20 The user account creation mechanism shall be extensible such that it will support the execution of additional tasks during user account creation as required by the COE and its segments. These tasks may include adding users to the DBMS, Profile Database, and DCE Registry and creating user's home directory.

Traceability:
Priority ???

3.2.1.21 Management Services shall create users such that it will support unitary login of the user.

Traceability:
Priority ???

3.2.1.22 The unitary login capability shall support a transparent, distributed login capability for all users.

Traceability:
Priority ???

3.2.1.23 Management Services shall provide a GUI-based capability for centralized user account modification in a heterogeneous environment with the capability to modify the following user parameters:

- Login name

  Traceability:
  Priority ???

- Password

  Traceability:
  Priority ???

- Home directory file server

  Traceability:
  Priority ???

- Group memberships

  Traceability:
  Priority ???

- Mail alias(es)

  Traceability:
  Priority ???

- Shell

  Traceability:
  Priority ???

- Other user information, e.g., user's real name, telephone

Traceability:
Priority ???

If the user's home directory file server is modified, the account modification mechanism shall create a new home directory on that server.

3.2.1.24 Management Services shall provide a GUI-based capability for centralized user account deletion in a heterogeneous environment. The user account deletion mechanism will provide the capability to reverse all actions associated with user account creation. The account deletion mechanism shall prompt for user home directory deletion, with a default of "no".

Traceability:
Priority ???

3.2.1.25 The user account deletion mechanism shall be extensible such that it will support the execution of additional tasks during user account deletion as required by the COE and its segments. These tasks may include deleting users from the DBMS, Profile Database, and DCE Registry and deleting user's home directory.

Traceability:
Priority ???

3.2.1.26 Management Services shall provide the capability to automatically distribute or make available user account information to a single host, a group of hosts or all hosts within the administrative domain.

Traceability:
Priority ???

3.2.1.27 Management Services shall provide a GUI-based capability for centralized group creation in a heterogeneous environment with the capability to modify the following group parameters:

- Unique group identifier (within administrative domain)

Traceability:
Priority ???

- Group name

Traceability:
Priority ???

- Members

Traceability:
Priority ???

The group creation mechanism shall not be capable of creating account groups as defined in the DII I&RTS.

3.2.1.28 Management Services shall provide a GUI-based capability for centralized group modification in a heterogeneous environment with the capability to modify the following group parameters:

- Group name

Traceability:
Priority ???

- Members

Traceability:
Priority ???

The group modification mechanism shall not be capable of modifying account groups as defined in the DII I&RTS.

3.2.1.29 Management Services shall provide a GUI-based capability for centralized group deletion in a heterogeneous environment. The group account deletion mechanism will provide the capability to reverse all actions associated with group account creation.

Traceability:
Priority ???

The group deletion mechanism shall not be capable of deleting account groups as defined in the DII I&RTS.

3.2.1.30 Management Services shall provide the capability to automatically distribute or make available group information to a single host, a group of hosts or all hosts within the administrative domain.

Traceability:

3.2.1.31 Management Services shall provide a GUI-based capability for centralized host definition in a heterogeneous environment with the capability to define the following host parameters:

- Hostname

  Traceability:
  Priority ???

- IP Address

  Traceability:
  Priority ???

- Hostname aliases

  Traceability:
  Priority ???

3.2.1.32 Management Services shall provide the capability to automatically distribute or make available host information to a single host, a group of hosts or all hosts within the administrative domain.

Traceability:
Priority ???

3.2.1.33 Management Services shall provide a GUI-based capability to install software resources and patches from a central location on a single host, a group of hosts or all hosts within the administrative domain.

Traceability:
Priority ???

3.2.1.34 The software installation mechanism shall be extensible such that it will support the execution of additional tasks during software installation as required by the COE and its segments. These tasks may include identification of the system functions of the software, associating those system functions with account groups and updating the profile database with new system functions.

Traceability:
Priority ???

3.2.1.35 Management Services shall provide a GUI-based capability to upgrade software resources and patches from a central location on a single host, a group of hosts or all hosts within the administrative domain.

Traceability:
Priority ???

3.2.1.36 The software upgrade mechanism shall be extensible such that it will support the execution of additional tasks during software upgrade as required by the COE and its segments. These tasks may include identification of the system functions of the software, associating those system functions with account groups and updating the profile database with new system functions.

Traceability:
Priority ???

3.2.1.37 Management Services shall provide a GUI-based capability to deinstall software resources and patches from a central location on a single host, a group of hosts or all hosts within the administrative domain.

Traceability:
Priority ???

3.2.1.38 The software deinstallation mechanism shall be extensible such that it will support the execution of additional tasks during software de-installation as required by the COE and its segments. These tasks may include removal of the system functions of the software from an account groups and updating the profile database.

Traceability:
Priority ???

3.2.1.39 Management Services shall provide a GUI-based capability for centralized distribution of files and file packages (including directories of files) from a central location to a single host, a group of hosts or all hosts within the administrative domain.

Traceability:
Priority ???

3.2.1.40 Management Services shall provide a GUI-based capability to centrally monitor and control print queues in a heterogeneous environment and perform the following administration tasks:

Traceability:
Priority ???

3.2.1.40a Management Services shall provide the capability to display the print queue.

Traceability:
Priority ???

3.2.1.40b Management Services shall provide the capability to start the print queue.

Traceability:
Priority ???

3.2.1.40c Management Services shall provide the capability to stop the print queue.

Traceability:
Priority ???

3.2.1.40d Management Services shall provide the capability to delete print jobs from the print queue.

Traceability:
Priority ???

3.2.1.40e Management Services shall provide the capability to prioritize print jobs in the print queue

Traceability:
Priority ???

3.2.1.40f Management Services shall provide the capability to move print jobs in the print queue.

Traceability:
Priority ???

3.2.1.40g Management Services shall provide the capability to move print jobs between print queues.

Traceability:
Priority ???

3.2.1.41 Management Services shall provide a GUI-based capability to centrally monitor and control printer in a heterogeneous environment and perform the following administration tasks:

3.2.1.41a Management Services shall provide the capability to start printers.

Traceability:
Priority ???

3.2.1.41b Management Services shall provide the capability to stop printers.

Traceability:
Priority ???

3.2.1.41c Management Services shall provide the capability to flush printers.

Traceability:
Priority ???

3.2.1.42 Management Services shall provide the capability to centrally create print queues in a heterogeneous environment within the administrative domain.

Traceability:
Priority ???

3.2.1.43 Management Services shall provide the capability to centrally delete print queues in a heterogeneous environment within the administrative domain.

Traceability:
Priority ???

3.2.1.44 Management Services shall provide the capability to create printer definitions for the printing system within the administrative domain with the capability to define the following parameters:

- Printer Name(s)

Traceability:
Priority ???

- Printer Type

Traceability:
Priority ???

- Print Server

Traceability:
Priority ???

- Printer Parameters (e.g., default, flow control)

Traceability:
Priority ???

3.2.1.45 Management Services shall provide the capability to modify printer definitions in the printing system within the administrative domain with the capability to define the following parameters:

- Printer Name(s)

Traceability:
Priority ???

- Printer Type

Traceability:
Priority ???

- Print Server

Traceability:
Priority ???

- Printer Parameters (e.g., default, flow control)

Traceability:
Priority ???

3.2.1.46 Management Services shall provide the capability to delete printer definitions from the printing system within the administrative domain. The printer deletion mechanism will provide the capability to reverse all actions associated with printer definition.

Traceability:
Priority ???

3.2.1.47 Management Services shall provide the capability to automatically distribute or make available printer information to a single host, a group of hosts or all hosts within the administrative domain.

Traceability:
Priority ???

3.2.1.48 Management Services shall provide a GUI-based capability for centralized monitor and control of processes in a heterogeneous environment and perform the following administration tasks:

Traceability:
Priority ???

3.2.1.48a Management Services shall provide the capability to display the status of processing resources.

Traceability:
Priority ???

3.2.1.48b Management Services shall provide the capability to identify active and failed processes.

Traceability:
Priority ???

3.2.1.48c Management Services shall provide the capability to terminate processes.

Traceability:
Priority ???

3.2.1.48d Management Services shall provide the capability to suspend processes.

Traceability:
Priority ???

3.2.1.48e Management Services shall provide the capability to resume processes.

Traceability:
Priority ???

3.2.1.48f Management Services shall provide the capability to send administrator-defined signals to processes, e.g., SIGHUP.

Traceability:
Priority ???

3.2.1.49 Management Services shall provide the capability to control disk resources and perform the following administration tasks:

3.2.1.49a Management Services shall provide the capability to allocate user disk space including setting quotas.

Traceability:
Priority ???

3.2.1.49b Management Services shall provide the capability to modify disk partitions.

Traceability:
Priority ???

3.2.1.49c Management Services shall provide the capability to mount file systems.
Traceability:
Priority ???

3.2.1.49d Management Services shall provide the capability to unmount file systems.
Traceability:
Priority ???

3.2.1.49e Management Services shall provide the capability to determine disk space usage.
Traceability:
Priority ???

3.2.1.49f Management Services shall provide the capability to determine disk space availability.
Traceability:
Priority ???

3.2.1.49g Management Services shall provide the capability to create file systems.
Traceability:
Priority ???

3.2.1.49h Management Services shall provide the capability to modify file systems.
Traceability:
Priority ???

3.2.1.49i Management Services shall provide the capability to create file system tables.
Traceability:
Priority ???

3.2.1.49j Management Services shall provide the capability to modify file system tables.
Traceability:
Priority ???

3.2.1.49k Management Services shall provide the capability to export file system tables.
Traceability:
Priority ???

3.2.1.50 Management Services shall provide the capability to specify a drift threshold for time synchronization across the administrative domain.
Traceability:
Priority ???

3.2.1.51 Management Services shall provide the capability specify a synchronization method (e.g., abrupt, increase rate) for time synchronization across the administrative domain.
Traceability:
Priority ???

3.2.1.52 Management Services shall provide the capability to monitor and control peripherals within the administrative domain (e.g., cdroms, printers, tape drives) and perform the following administration tasks:

3.2.1.52a Management Services shall provide the capability to allocate access to peripherals.
Traceability:
Priority ???

3.2.1.53 Management Services shall provide the capability for centralized reboot and change of run state of a single host, a group of hosts or all hosts within the administrative domain.
Traceability:
Priority ???

3.2.1.54 Management Services shall provide a GUI-based capability to centrally monitor and control system and application log files within the administrative domain and perform the following administration tasks:

3.2.1.54a Management Services shall provide the capability to view log files.
Traceability:
Priority ???

3.2.1.54b Management Services shall provide the capability to purge log files.
Traceability:
Priority ???

3.2.1.54c Management Services shall provide the capability to archive log files to a selected storage medium.
Traceability:
Priority ???

3.2.1.54d Management Services shall provide the capability to print logs files to a selected printer.
Traceability:
Priority ???

3.2.1.54e Management Services shall provide the capability to compress log files.
Traceability:
Priority ???

3.2.1.54f Management Services shall provide the capability to control the size of the log files.
Traceability:
Priority ???

3.2.1.54g Management Services shall provide the capability to enable/disable logging.
Traceability:
Priority ???

3.2.1.54h Management Services shall provide the capability to search log files.
Traceability:
Priority ???

3.2.1.55 Management Services shall provide the capability to detect and identify all network addressable managed hardware resources within each management domain. This shall include, at a minimum, the following attributes:

- IP Address
  Traceability:
  Priority ???
- Name
  Traceability:
  Priority ???
- Location to nearest router
  Traceability:
  Priority ???
- Other information as available
  Traceability:
  Priority ???

3.2.1.56 Management Services shall provide the capability to identify all managed software resources (e.g., segments) within each management domain. This shall include, at a minimum, the following attributes:

- Name

  Traceability:
  Priority ???

- Installation Location (e.g., installed host)

  Traceability:
  Priority ???

- Type

  Traceability:
  Priority ???

- Version and Release Number

  Traceability:
  Priority ???

- Patch Number

  Traceability:
  Priority ???

- Other information as available

  Traceability:
  Priority ???

3.2.1.57 Management Services shall provide the capability to create a diagrammatic representation of the interconnected network resources within each management domain.

Traceability:
Priority ???

3.2.1.58 Management Services shall provide the capability to update the diagrammatic representation of the interconnected network resources within each management domain.

Traceability:
Priority ???

3.2.1.59 Management Services shall provide the capability to display and print a diagrammatic representation of the interconnected network resources within each management domain.

Traceability:
Priority ???

3.2.1.60 Management Services shall provide the capability to detect and modify the configuration of hardware and software resources from a central location within the management domain. The manager shall be capable of detecting and modifying the attributes of managed objects implemented and used by host and network resources in the management domain. Each manager agent residing on a workstation, server or network device shall be capable of responding to requests from the manager to return the value of the attribute stated in the manager's request and to modify the current value of the attribute stated in the request. Managed objects shall be defined and their attributes managed in accordance with Internet Request for Comment (RFC) 1514 (Host Resources Management Information Base (MIB)) and RFC 1213 (MIB II).

Traceability:
Priority ???

RFC 1514 defines managed objects for workstations and servers. Workstations and servers in the DII COE shall implement the following groups of managed objects.

- Mandatory Managed Groups
  - Host Resources System Group
  - Host Resources Storage Group
  - Host Resources Device Group
- Optional Managed Groups
  - Host Resources Running Software Group
  - Host Resources Running Software Performance
  - Host Resources Installed Software Group

RFC 1213 defines the MIB II for network management protocols in TCP/IP-based networks. The MIB is defined in terms of groups of managed objects. If the semantics of a group is applicable to an implementation (i.e., a network device), then the devices shall implement all objects in that group. (This is guidance for managed agents, the managing server must implement all groups.)

For network devices, the managed groups are: System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP, Transmission and SNMP.

3.2.1.61 Management Services shall provide the capability to view the network names and addresses of all managed objects in the management domain.

Traceability:
Priority ???

3.2.1.62 Management Services shall provide the capability to assign network names and addresses of all managed objects in the management domain.

Traceability:
Priority ???

3.2.1.63 Management Services shall provide the capability to modify network names and addresses of all managed objects in the management domain.

Traceability:
Priority ???

3.2.1.64 Management Services shall provide the following automated capabilities to support the maintenance of the managed hardware inventory.

3.2.1.64a Management Services shall provide the capability to create information in a database of the managed hardware inventory to include, at a minimum, the following parameters:

- Manufacturer

Traceability:
Priority ???

- Type

Traceability:
Priority ???

- Model

Traceability:
Priority ???

3.2.1.64b Management Services shall provide the capability to modify information in a database of the managed hardware inventory to include, at a minimum, the following parameters:

- Manufacturer

Traceability:
Priority ???

- Type

Traceability:
Priority ???

- Model

Traceability:
Priority ???

3.2.1.64c Management Services shall provide the capability to delete information in a database of the managed hardware inventory to include, at a minimum, the following parameters:

- Manufacturer

Traceability:
Priority ???

- Type

Traceability:
Priority ???

- Model

Traceability:
Priority ???

3.2.1.64d Management Services shall provide the capability to report the status of the managed hardware inventory within the management domain on request. Separate reports shall be available for each type of equipment.

Traceability:
Priority ???

3.2.1.64e Management Services shall provide the capability to send an alert in accordance with the DII Alerts SRS automatically when managed hardware inventory levels fall below a manually set threshold. The default threshold value shall be one spare unit.

Traceability:
Priority ???

3.2.1.65 Management Services shall provide the capability to monitor inventory status on software (to include versions, types and numbers) at any given time by use of automated inventory control software.

Traceability:
Priority ???

3.2.1.66 Management Services shall provide the capability to report inventory status on software (to include versions, types and numbers) at any given time by use of automated inventory control software.

Traceability:
Priority ???

MS 3.2.2 Fault Management

Fault management encompasses the need for a proactive capability to monitor, detect, identify, analyze, isolate and correct problems related to abnormal behavior of managed resources within DII. An important design consideration of DII is that it will not contain any "single points of failure."

3.2.2.1 Agents shall report changes of status of managed objects to the manager of the associated management domain.

Traceability:
Priority ???

3.2.2.2 Management Services shall provide the capability to detect the loss of managed objects within each management domain.

Traceability:
Priority ???

3.2.2.3 Management Services shall provide the capability to locate a failed managed object within a LAN segment (i.e., to the nearest router).

Traceability:
Priority ???

3.2.2.4 Management Services shall provide the capability to disable failed or malfunctioning managed objects.

Traceability:
Priority ???

3.2.2.5 Management Services shall provide the capability to disable routers and bridges in order to isolate LAN segments.

Traceability:
Priority ???

3.2.2.6 Management Services shall provide the capability for centralized backup of the system or selected files on the system to an off-line selectable device in an automated mode.

Traceability:
Priority ???

3.2.2.7 Management Services shall provide the capability for centralized backup of the system or selected files on the system to an off-line selectable device in a manual mode.

Traceability:
Priority ???

3.2.2.8 Management Services shall provide the capability for centralized restore of the system or selected files on the system from an off-line selectable device.

Traceability:
Priority ???

MS 3.2.3 Performance Management

Monitoring and controlling the quality of network communications and ensuring satisfactory performance of system resources is a primary thrust of the Management Services. This process involves the monitoring and analyzing, tuning and controlling, and reporting on network and information system components to include the system as one entity. The monitoring and analyzing functions include establishing the monitoring environment, the performance indicators, and the generation of appropriate reports. Tuning and controlling functions include activation of controls in order to fine tune the performance of the network and information systems. Recognizing and diagnosing the performance deficiencies are considered to be a fundamental requirement for the performance of the system. Reports being generated can include monitoring, tuning, tracking, and trend analysis.

Performance management includes those functions necessary to ensure optimum performance of the system. This, of necessity, entails the capability to monitor and adjust each manageable object in the management domain.

3.2.3.1 Management Services shall provide the capability to retrieve usage-related attributes from managed objects . This shall include, as a minimum, the following attributes:

- Processor load in terms of percent of maximum capacity

Traceability:
Priority ???

- Disk use in terms of percent of maximum capacity

Traceability:
Priority ???

- Memory use in terms of percent of maximum capacity

  Traceability:
  Priority ???

- Network load in terms of average and instantaneous bytes per second

  Traceability:
  Priority ???

3.2.3.2 Management Services shall provide the capability to modify managed object attributes. This shall include, as a minimum, the following attributes:

- Routing tables

  Traceability:
  Priority ???

- Buffer sizes

  Traceability:
  Priority ???

- Timers

  Traceability:
  Priority ???

- Swap Space

  Traceability:
  Priority ???

3.2.3.3 Management Services shall provide the capability to move files and applications among the servers within the management domain.

Traceability:
Priority ???

3.2.3.4 Management Services shall generate an alert in accordance with the Alerts SRS when the physical disk usage in the management domain reaches a definable threshold set by the operator. The threshold shall have a default value of 80%.

Traceability:
Priority ???

3.2.3.5 Management Services shall provide the capability to generate a summary of performance and utilization of each managed object within the management domain.

Traceability:
Priority ???

3.2.3.6 Management Services shall provide the capability for a single user to authenticate (via the GUI-based login mechanism) and be presented with a list of valid profiles (via the GUI-based profile selection mechanism) in the DII COE within ten (10) seconds.

Traceability:
Priority ???

3.2.3.7 Management Services shall provide the capability for a single user to select one or more profiles (via the GUI-based profile selection mechanism) and be presented with the appropriate session icons (via the common desktop environment) in the DII COE within twenty (20) seconds.

Traceability:
Priority ???

3.2.3.8 Management Services shall provide the capability for a single user to change their profile(s) (via the GUI-based profile change mechanism) and be presented with the appropriate session icons (via the common desktop environment) in the DII COE within twenty (20) seconds.

Traceability:
Priority ???

3.2.3.9 Management Services shall provide the capability for a single user to launch a profile-based application (via the common desktop environment) and be presented with the application in the DII COE within five (5) seconds.

Traceability:
Priority ???

3.2.3.10 Management Services shall provide the capability for a single user to logout of their user session (via the GUI-based logout mechanism) in the DII COE within ten (10) seconds.

Traceability:
Priority ???

3.2.3.11 Management Services shall provide the capability for an administrator to create a single user in the DII COE within four (4) minutes. Creating a user includes defining the following parameters in the appropriate files and databases in the DII COE:

- Unique user identifier

  Traceability:
  Priority ???

- Login name

  Traceability:
  Priority ???

- Initial password

  Traceability:
  Priority ???

- Home directory file server

  Traceability:
  Priority ???

- Group memberships

  Traceability:
  Priority ???

- Mail alias(es)

  Traceability:
  Priority ???

- Shell

  Traceability:
  Priority ???

- Other user information, e.g., user's real name, telephone

  Traceability:
  Priority ???

- Profiles

  Traceability:
  Priority ???

- Other parameters as required by the DII COE and its segments (e.g., DBMS registry, DCE registry)

Traceability:
Priority ???

3.2.3.12 Management Services shall provide the capability for an administrator to create a single profile in the DII COE within two (2) minutes. Creating a profile includes defining the following parameters in the appropriate files and databases in the DII COE:

- Unique profile name

  Traceability:
  Priority ???

- Account Group

  Traceability:
  Priority ???

- System Function(s)

  Traceability:
  Priority ???

- Other parameters as required by the DII COE and its segments (e.g., DBMS permissions, DCE access controls)

  Traceability:
  Priority ???

MS 3.2.4 Security Management

DII Security Management is derived from national security policy and DII mission requirements. The Management Services safeguard against various real threats such as unauthorized information access, expanding authorized access without appropriate authorization, information destruction, denying service, etc. The Management Services will operate in concert with the security management procedures of those systems supporting the DII, which can be the source of external threats. Management Services must cover all areas of security to include authentication, access control, encryption, and the ensuing audit trails. Authorized users will monitor and control the mechanisms which exist to protect network resources and user information, using the automated tools provided by Management Services.

Security management systems include functionality for key management, access control and audit. The centralized control of these functions may be implemented either in a security management center on one hardware platform, or in distributed security management centers, each covering a specific management function. In either case, the scope of security management will be constrained to be consistent with the management domains.

The security requirements outlined within this document are a reflection of the DII security policy and are applicable in assisting the DII Security Administrator in completing his/her operational mission through system availability, confidentiality, accountability and integrity.

Information system security encompasses four security services:

Accountability: The property that enables activities on a system to be traced to individuals who may then be held responsible.

Availability: The property of system resources and information being accessible and usable upon demand by an authorized entity.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity: The property that information has not been altered or destroyed in an unauthorized manner.

MS 3.2.4.1 Accountability

3.2.4.1.1 Management Services shall provide the a GUI-based capability to check whether or not the DII COE components are operating in a secure mode in accordance with the DII Security Requirements and to perform the following administrative tasks:

3.2.4.1.1a Management Services shall provide the capability to ensure security relevant system files and directories do not have dangerous access permissions (e.g., world writable or world readable).

Traceability:
Priority ???

3.2.4.1.1b Management Services shall provide the capability to examine the boot commands to ensure that files or paths referenced are not world writable.

Traceability:
Priority ???

3.2.4.1.1c Management Services shall provide the capability to ensure system devices are not world writable or world readable and that file systems have not been shared without any restrictions.

Traceability:
Priority ???

3.2.4.1.1d Management Services shall provide the capability to analyze the local or network user database and flag accounts with improperly constructed passwords in accordance the DII Security SRS, improper number of fields, non-unique user identifiers, and blank lines.

Traceability:
Priority ???

3.2.4.1.1e Management Services shall provide the capability to analyze the local or network group database and flag accounts with improperly constructed passwords in accordance the DII Security SRS, improper number of fields, non-unique group identifiers, blank lines and groups with duplicative members.

Traceability:
Priority ???

3.2.4.1.1f Management Services shall provide the capability to analyze trusted access to the system.

Traceability:
Priority ???

3.2.4.1.1g Management Services shall provide the capability to examine user home directories and specific files in each home directory to ensure they are not world writable.

Traceability:
Priority ???

3.2.4.1.1h Management Services shall provide the capability to analyze the protection configuration provided by the system using a rule based expert system.

Traceability:
Priority ???

3.2.4.1.1i Management Services shall provide the capability to check passwords against various dictionaries and certain algorithmic permutations to identify passwords that are easy to guess using a trial and error methodology. The dictionaries and permutations to use shall be configurable.

Traceability:
Priority ???

3.2.4.1.1j Management Services shall provide the capability to determine the version level of important system binaries and identify those that have not had the most recent security patches applied.

Traceability:
Priority ???

3.2.4.1.1k Management Services shall provide the capability to check for unexpected file system corruption or security breaches using Cyclic Redundancy Checks (CRCs) and changes to a file's inode attributes.

Traceability:
Priority ???

3.2.4.1.1l Management Services shall provide the capability to measure intrusion detection by reporting changes to a file's RSA MD5 encryption signature.

Traceability:
Priority ???

3.2.4.1.2 Management Services shall provide the capability to identify each authorized DII user with a unique identifier (e.g., username) within the management domain.

Traceability:
Priority ???

3.2.4.1.3 Management Services shall provide the capability to enable/disable security-relevant audit events within the administrative domain.

Traceability:
Priority ???

3.2.4.1.4 Management Services shall provide a GUI-based capability for centralized audit reduction in a heterogeneous environment with the capability to selectively filter the audit records in accordance with the DII Security Requirements.

Traceability:
Priority ???

3.2.4.1.5 Management Services shall provide a GUI-based capability for centralized audit trail management with the capability to perform the following administrative tasks:

3.2.4.1.5a Management Services shall provide the capability to view the raw audit trail.

Traceability:
Priority ???

3.2.4.1.5b Management Services shall provide the capability to view the reduced audit trail.

Traceability:
Priority ???

3.2.4.1.5c Management Services shall provide the capability to backup the audit trail to a selectable device.

Traceability:
Priority ???

3.2.4.1.5d Management Services shall provide the capability to restore the audit trail from a selectable device

Traceability:
Priority ???

3.2.4.1.5e Management Services shall provide the capability to archive the audit trail to a selectable device.

Traceability:
Priority ???

3.2.4.1.5f Management Services shall provide the capability to delete the audit trail. The audit deletion capability will not delete the audit trail without verifying the action with the administrator.

Traceability:
Priority ???

3.2.4.1.6 Management Services shall provide a GUI-based capability to assign passwords to users.

Traceability:
Priority ???

MS 3.2.4.2 Availability

3.2.4.2.1 Management Services shall support trusted roles as defined in the DII Security Requirements.

Traceability:
Priority ???

3.2.4.2.2 Management Services shall limit the system functions assigned to a trusted role to those required to perform the trusted role effectively as defined in the DII I&RTS.

Traceability:
Priority ???

3.2.4.2.3 Management Services shall prohibit security relevant functions from being assigned to non-trusted roles. Security relevant functions include those functions which may affect the implementation of the security policy within the DII COE.

Traceability:
Priority ???

MS 3.2.4.3 Confidentiality

3.2.4.3.1 Management Services shall provide a GUI-based capability to set the access permissions (e.g., read, write, execute, control, delete) of system resources (e.g., files, directories and applications), and to associate those privileges with specific users.

Traceability:
Priority ???

3.2.4.3.2 Management Services shall provide a GUI-based capability to set the access permissions (e.g., read, write, execute, control, delete) of system resources (e.g., files, directories and applications), and to associate those privileges with specific groups.

Traceability:
Priority ???

3.2.4.3.3 Management Services shall provide a GUI-based capability to set the ownership of system resources (e.g., files, directories and applications).

Traceability:
Priority ???

3.2.4.3.4 Management Services shall provide the capability to manage sensitivity labels and handling caveats used in marking printed output with sensitivity labels and handling caveats.

Traceability:
Priority ???

3.2.4.3.5 Management Services shall provide the capability to enable or disable marking printed output with sensitivity labels and handling caveats.

Traceability:
Priority ???

3.2.4.3.6 Management Services shall provide a GUI-based capability for creating a set of authorized sensitivity labels and handling caveat values for use in marking printed output.

Traceability:
Priority ???

3.2.4.3.7 Management Services shall provide a GUI-based capability for modifying the set of authorized sensitivity labels and handling caveat values that are used in marking printed output.

Traceability:
Priority ???

3.2.4.3.8 Management Services shall provide a GUI-based capability for deleting of the set of authorized sensitivity label and handling caveat values that are used in marking printed output.

Traceability:
Priority ???

MS 3.2.4.4 Integrity

3.2.4.4.1 Management Services shall provide the capability to scan the DII COE for known malicious software, e.g., worms, viruses, trojan horses.

Traceability:
Priority ???

3.2.4.4.2 Management Services shall provide the capability to remove from the DII COE known malicious software, e.g., worms, viruses, trojan horses.

Traceability:
Priority ???